IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 20-94
	)	
JUSTIN SEAN JOHNSON	)	Hornak, J.

SENTENCING MEMORANDUM OF THE UNITED STATES

AND NOW comes the United States of America, by its attorneys, Stephen R. Kaufman, Acting United States Attorney for the Western District of Pennsylvania, and Gregory C. Melucci, Assistant United States Attorney for said District, and submits the following Sentencing Memorandum.

Summary

In January 2014, UPMC computer servers in Pittsburgh were "hacked" by an assailant whose aim was to steal, and later solicit on the dark web sensitive personal information (PII) belonging to tens of thousands of past and present UPMC employees. It may have been the largest individual hack of PII from a Pittsburgh based institution in the history of this District. Virtually no employee in the HR payroll system of UPMC was spared. UPMC confirmed that over 60,000 identities, including highly sensitive payroll, wage, and tax identifiers were stolen by the hacker. Soon after the intrusion, the anxiety to employees and UPMC over the use of their PII manifested when hundreds of false federal income tax returns were electronically filed using the PII of UPMC employees, claiming approximately $2.9 million in unlawful refunds monetized in the form of Amazon.com gift cards used by conspirators to purchase hundreds of thousands of dollars in high end electronics from Amazon shipped to Venezuela. Several foreign conspirators were captured and convicted. The monetization of the PII continued as investigators tracked the hacker through the dark internet underworld, soliciting the same PII of UPMC workers to buyers with sinister motives.

Meanwhile, the hacker employed sophisticated "cloaking" tools, keeping himself virtually invisible from trained investigators while he marketed the PII to underworld buyers. Using aliases such as "The Dearth Star" and "Dearthy Star" (hereafter DS), for several years the hacker lived anonymously in the underworld marketing UPMC and other PII to whomever would buy. Staying close on the hacker's trail, investigators caught a break in 2014 when the stolen PII appeared on the computer of a buyer who revealed his interactions with the "Dearth Star" on the dark web. Persistent investigators followed DS through underworld forums and in encrypted chat communications soliciting PII, and offering criminal advice to buyers. In late 2016, DS slipped up, revealing a critical user identifier to a buyer. Investigators later seized upon it and the hacker, which led to the identity of the defendant, Justin S. Johnson, as the UPMC hacker and dark web underworld salesman of bulk PII. The "masked hacker" was uncovered, and in June 2019, was arrested while living out of a short-term rental unit stop in Michigan. All told, the evidence seized from Johnson revealed just how significant he was in the dark web soliciting stolen identities. It also revealed a vast collection of underworld data, demonstrating that Johnson's prey was not limited to UPMC.

Now is the moment when Johnson faces the consequences of his criminal behavior. The statutory maximum sentence for the two counts of conviction is 84 months incarceration; the USSG calculation is slightly less (in combination with the statutorily mandated 24 months for aggravated identity theft) or 70-81 months incarceration. If there is a case to be made for a statutory maximum sentence, for the reasons below, this is it.

The Nature and Circumstances of the Offense Warrant a Statutory Maximum Sentence

"Cybersleuthing" is probably the most challenging federal prosecution. Investigators may spend hundreds of hours, and prepare mounds of legal process chasing shadows and underworld ghosts to identify a culprit. It's fraught with ups and downs, false leads, brick walls, and traps.

Often cybercrooks can go years living anonymously. However, the reward, like to goldminers in the 1800's, is worth the mining. To investigators, the chase for DS was equally challenging, composed of almost one-half decade-of tireless pursuit of likely the largest institutional hacker in the Western District.

The Indictment details just how calculated Justin Johnson was in planning the assault on UPMC servers. In private chats in 2013, Johnson teased his plan to "acquire" and to "sell" PII, and to "be rich by the end of the year." To do so, he needed to "play with peoplesoft" – "HR in a box" as he called it. The UPMC hack was premeditated. Indeed, investigators years later uncovered Johnson's "PeopleSoft expertise," having studiously searched for Peoplesoft over 1,100 times on his computer. In his "LinkedIn" profile and on his resumé, he bragged about his expertise in understanding, installing and implementing PeopleSoft. Investigators also uncovered "The Hacker Playbook2: Practical Guide to Penetration Testing" on his electronics. His intrusion into the UPMC Oracle-PeopleSoft controlled network resulted from his understanding of PeopleSoft network systems and in technical manuals. With this knowledge, DS somehow figured a way to work around PeopleSoft's security, and in January and February 2014, surreptitiously by using anonymizing TOR software, targeted and hacked a treasure trove of PII at the heart of one of the largest health care employers in the nation. Only days later, Johnson, using the underworld moniker "The Dearth Star", solicited "W-2 packs" including "DOB" and "SSN" of victim identities "originating from Pennsylvania." Buyers of this stolen UPMC data quickly monetized it through nearly 1,200 false federal income tax returns and Amazon tax refund gift cards into $340,000 dollars in illegally-obtained Amazon electronic merchandise shipped to cities in Venezuela. There, the buyers of the Amazon merchandise were identified, resulting in at least two federal convictions. The false returns cost the IRS $1.7 million dollars in unlawful tax refunds.

Johnson's early success encouraged him to find other ways to solicit the stolen UPMC data. In 2015 after a short respite, DS proudly returned to the dark underworld bragging of owning a collection of "tens of thousands" of "fresh names, SSN and bank routing" information. DS was not interested in small buyers. He had "swiped" employers with "10,000+ employees" by "raiding the HR systems of an institution with tens of thousands of names" and looking for bulk buyers. Surfing the dark web forums such as Alpha Bay, DS boasted his success, selling institutionally-hacked PII- of "45,000 fresh names/addresses/DOB/SSN." He touted his success hacking "THREE colleges" including student academic systems protected with "shitty/default passwords." Not limiting his victims to only institutional employees, he even advertised for sale "many profiles of college students and prospective college students (and sometimes their parents) with an IRS verified 2015 AGI."

Records seized from storage lockers in Michigan after Johnson's arrest confirmed DS' vast hacking capabilities: forensic reviews of laptop computers and hard drives uncovered files holding 89,000 pieces of PII belonging to employees, students, and hospital patients at Butler University, Daytona State College and Palomar College, as well as employee (and patient) PII of healthcare providers Pruitt Health Care in Georgia, and Lexington Medical Center in in South Carolina. DS' electronics also revealed PII hacked from New Jersey University, and George Fox University in Oregon. Not surprisingly, the common denominator was a PeopleSoft HR network. DS was regularly followed on the dark web networks by shoppers who posted positive feedback such as "nice product," "good seller," or "a straightforward seller" and even going "way out of his way to help" customers.

DS's sophistication and hacking capabilities enabled him to avoid detection and capture for several years. Forensic investigators determined that DS used obfuscating tools such as the TOR network to disguise his infiltration and exfiltration of massive amounts of PII from UPMC,

which frustrated law enforcement efforts. He also lived anonymously on dark web trading forums using aliases and encrypted chat communication services to solicit PII. He accepted only cryptocurrency Bitcoin which he held in multiple Bitcoin exchanges such as "Coinbase" and "Localbitcoins." In the end, ironically the Bitcoin account would expose him.

During this time, investigators later confirmed that he traveled extensively throughout the United States to Chicago, San Francisco, Washington D.C. and elsewhere, frequently by Amtrak. He worked a as a "bug bountier" identifying bugs and vulnerabilities in company networks, and then demanding payment in return. For a while in 2018 and 2019 he lived in France.

At some point, like Ponzi schemers, hackers know that law enforcement will catch up and find them. However, during the window of time before capture, DS was able to capitalize on the moment and do as much damage as possible. Here, in the later years before capture, DS' chats reveal more brazen and aggressive efforts to solicit PII, but oddly, financial records recovered by investigators do not show that his hacking career was too lucrative.

The History and Characteristics of Johnson Reveal His Dangerous Hacking Capabilities.

Johnson's hacking successes are explained by a combination of extremely savvy understanding of software systems, persistence, and opportunity. Johnson is only 30, with little college education. Born and raised in Detroit, after high school he attended several community colleges but never graduated. His employment history is equally sporadic and incomplete: between 2009 until his arrest in 2020, he held mostly part-time jobs in Florida and Michigan, earning "part-time" income. In 2016 he started the "bug bounty" career, likely learning essential tools to move up and into the hacker underworld. The part-time work lifestyle afforded him plenty of spare time to investigate culpabilities in company networks and refine his hacking skills. Despite his incomplete formal education, his resumé reveals his sophistication in offering services in cloud-based Linux systems administration and technical IT services to companies. He offered

"tax preparation" expertise to the public on chat rooms such as Reddit, and at one point even obtained a tax preparer PTIN for himself. On the dark webs, he regularly chatted with other hackers, exchanging tools and tips.

Meanwhile, Johnson paid careful attention to the happenings of the related cases as the paranoia of being detected gripped him. Forensic records of public records show that he regularly searched Pacer public record for his name, and developments in related cases *of U.S. v Yoandy Perez Llanes, and U.S. v. Justine Tollefson*. He downloaded many of the court documents. He also viewed dockets from other federal cybercrime cases as well. He frequently "googled" terms such as "NCIC warrant", "how to find out if you are indicted," "federal indictments" and "criminal complaints." In Reddit.com he discussed FBI arrests. His searches became more focused in 2019, checking "FBI name checks" "federal crimes" and arrests in other countries. His searches also included stolen identity refund fraud, IRS tax scams, and hacker sentences.

The massive amount of PII recovered from seized electronics he stored reflect not only his dangerous capabilities as a cyberthief, but also his detailed methodology and crafting needed for his cyberfraud-skills. One wonders how he useful he might have been had he redirected his skills lawfully.

Johnson could not resist temptation even when offered a legitimate job. In July, 2019, he responded to an ad seeking a "computer technician responsible for hard drive wiping." Johnson, whose duties included to wipe, or erase, the hard drives of old computer systems from educational institutions and other companies was fired from the job after scarcely four months because the owner of the company caught Johnson attempting to access data on the hard drives before "wiping" them.

Either A "Top-End" Guidelines Sentence or Statutory Maximum Sentence is Substantively Reasonable, Reflecting the Seriousness of the Crimes, Affording Adequate Deterrence, and Protecting the Public.

The United States agrees with the USSG calculation in the PSR. The guideline calculation for Count 1, Conspiracy to Defraud the U.S. is 46-57 months driven by the tax loss to the Treasury of approximately $2.9 million dollars. Count 39, Aggravated Identity Theft, is a mandatory 24 month sentence pursuant to 18 U.S.C. Sec. 1028A(1), which must, by statute, be served consecutively to the sentence imposed on any other sentence. Id. 1028A(b)(2). Consequently, a reconfigured overall sentence is 70-81 months incarceration. Of course, the statutory maximum sentence is 84 months incarceration. In the recommendation of the United States, a sentence of 81-84 months is a substantively reasonable sentence. The Department of Justice has often emphasized the serious impact of cybercrime to Americans.

"The seriousness of cyber crimes and identity theft to the public cannot be understated. Cyber-enabled attacks are exacting an enormous toll on American businesses, government agencies, and families. Computer intrusions, cybercrime schemes, and the covert misuse of digital infrastructure have bankrupted firms, destroyed billions of dollars in investments, and helped hostile foreign governments launch influence operations designed to undermine fundamental American institutions. The Department of Justice's primary mission is to keep the American people safe. We play a critical role in the federal government's shared effort to combat malicious, cyber-enabled threats." *see*, "Report of the U.S. Attorney General's Cyber-Digital Task Force" July, 2018.

The hack by Johnson into UPMC computer networks and the multi-year investigation by skilled criminal investigators demonstrates just how serious and challenging cybercrime intrusion investigations have become. Johnson's use of obfuscating infiltration tools such as the TOR

browser, encrypted chat communications, and trading in crypto-currency enabled him not only to perpetrate the fraud, but empowered him to hack with impunity and to steal identities.

Identity theft is a pervasive and growing problem for Americans, causing both financial and emotional distress to victims. Statistics show that in 2018, an estimated 23 million persons, or about 9% of all United States residents age 16 or older reported that they had been victims of identity theft during the prior 12 months. Five percent of residents age 16 or older had experienced at least one incident involving the misuse of an existing credit card, and 4% had experienced the misuse of an existing bank account. Financial losses due to identity theft totaled $15.1 billion. Victims of new account misuse (15%) and personal information misuse (17%) were more likely to experience severe emotional distress. *see*, "Report on Identity Theft", Bureau of Justice Statistics, April, 2021.

That Johnson individually was able to amass an enormous collection of PII reveals how much damage one hacker can do to the public. The investigation uncovered at least 60,000 pieces of PII from UPMC, and 89,000 pieces of PII recovered from his electronic devices hacked from other institutions. Of course, this is just what investigators were able to recover. Certainly, given Johnson's proclivity to hack, more may have existed unknown to investigators.

Serious crimes of course deserve serious punishments. Nationally, federal courts have routinely sentenced cybercriminals to lengthy sentences, largely motivated by factors such as deterrence and the need to protect the public from further crimes by the defendant. see, *U.S. v. Kolpakov*, 19-159 (WDWA) (conspiracy to commit computer hacking resulting from breach of point-of-sale systems resulted in 120 month sentence); *U.S. v. Nikulin*, 2020 U.S. Dist. LEXIS 182234 (NDCA) (computer intruder and aggravated ID thief sentenced to 88 months incarceration and 1 million in restitution); *U.S. v. Hammond*, 2013 U.S. Dist. LEXIS 23992 (SDNY) (computer hacker sentenced to maximum 120 months incarceration); *U.S. v. Seleznev*, 2016 U.S. Dist. LEXIS

47356 (WDWA) (major Russian hacker sentenced to 27 years for sophisticated hacking); *U.S. v. Rainey*, 480 Fed. Appx. 842 (6th Cir. 2012) (number of victims, deterrence and need to protect public warranted maximum sentence).

Johnson is only 30 years old. Statistics indicate that persons in his age group are approximately 45% likely to recidivate within the first 2 years of release. *see*, "2018 Update of Prisoner Recidivism," Bureau of Justice Statistics, May, 2018. He has had a sporadic employment history, and his personal life has been unstable. Since 2013, he has never reported more than $7,000 in income. In 2019 he was hired by FEMA as a contract employee and wrote "homeless" for his residency on his application. For months leading to his arrest, he lived out of his car at a rest stop off I-94 near Ann Arbor, Michigan. Unless he receives significant rehabilitative help while incarcerated, when released, he is likely to resort to the easiest route to survive by doing what he does best-hacking networks. Consequently, a lengthy prison sentence will give him the opportunity to reflect on the harm he caused, just punishment for the serious harm caused to UPMC and its employees-and thousands of others-and hopefully deter him from future crimes to the public.

Respectfully submitted,

STEPHEN R. KAUFMAN
Acting United States Attorney

/s/ Gregory C. Melucci
GREGORY C. MELUCCI
Assistant United States Attorney
Joseph F. Weis, Jr. U.S. Courthouse
700 Grant Street, Suite 4000
Pittsburgh, Pennsylvania 15219
(412) 644-3500 (Phone)
(412) 644-4549 (Fax)
Gregory.Melucci@usdoj.gov
PA ID No. 56777